UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,747	10/31/2001	Richard Paul Tarquini	10014006-1	4897

7590 01/26/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 01/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/003,747
Filing Date: October 31, 2001
Appellant(s): TARQUINI, RICHARD PAUL

James Baudino
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/9/2005 appealing from the Office action mailed 8/3/2005.

(1) Real Party in Interest

The present application is assigned to Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,279,113 B1	Vaidya, Vimal	8-2001
6851061	Holland,III et al.	1-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

(a) Claims 1, 5-9, 15-16 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,279,113 B1 to Vaidya.

(b) Claims 2-4, 10-13, 17-19 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,279,113 B1 to Vaidya in view of U.S. Patent 6, 851, 061 B1 to Holland III et al.

(10) Response to Argument

(a) Appellant's arguments regarding Claim 1-13, 15 and 16 are not persuasive. As Vaidya discloses the monitoring of all seven OSI network layer, which includes application, transport, and network see Col 4 Ln 28-31 & Col 7 Ln 18-24. And further it is commonly known in the art that the first layer of OSI model through which communication(data flow) occurs is application, then presentation, then session, then transport, then network, then data link and finally physical. And Vaidya discloses of monitoring of all of seven of these layers including monitoring of application layer see Col 9 Ln 3-20; monitoring of transport layer see Col 8 Ln 40-56; monitoring of network layer see Col 5 Ln 5-26. And the appellant are merely selected three of the seven layers disclosed by Vaidya in the order already commonly known.

The Appellant's arguments regarding monitoring layer data by different layers of an intrusion prevention system is disclosed by Vaidya see discussion above. And further Vaidya mentions the timer/counter being used for application monitoring see Col 9 Ln 3-18 & Col 8 Ln 16-25(number of accesses in a certain period of time);a virtual processor for extracting the transport information see Col 7 Ln 18-24 and also an register cache being used to store and monitor transport data Col 8 Ln 40-53; data collector monitoring of network data see Col 6 Ln 57-63. And further Vaidya mentions the three types of signature based IDS present in his invention sequential, simple and timer-counter based see Col 3 Ln 66- Col 4 Ln 26(i.e. sequential representing the transport layer monitoring with cache, timer-counter representing the application layer monitoring with threshold, and simple representing the monitoring of network data and the instructions sent). And Vaidya discloses the sequential IDS being used to analyze and compare signature profile stored in cache containing transport data see Col 11 Ln 33-51; a timer/counter based IDS to monitor the application see Col 9 Ln 66-Col 10 Ln 15; a simple based IDS based on simple instructions to monitor for network data see Col 11 Ln 66-Col 12 Ln 10. Thus, Vaidya effectively discloses the monitoring of three layers as the instant invention with different layers in the intrusion detection system as shown by the different components used to monitor the different layers.

(b) Appellant's arguments regarding Claim 17-19 are not persuasive. As Holland discloses the layers having drivers see Col 5 Ln 61-67 and further the drivers being in

kernel space see Col 5 Ln 35-46 & Fig. 3 item 52 & Col 5 Ln 1-7. And further Holland discloses the media access control driver and intrusion prevention system transport service provider layer see Col 5 Ln 47-60, where Holland mentions TCP/UDP data being shimmed. And Holland also discloses the media access control driver see Col 4 Ln 52-67. And the drivers and intrusion prevention system transport service provider layer being part of IP stack(network stack) of operating system see Fig. 3 item 68 & Fig. 4 item 81-83

(c) Appellant's correctly points out Claim 14 is not listed in the rejection. There seems to be an typographical error it should have been rejected along the same lines as Claim 5 included in the Final rejection dated 8/3/2005.

For a more detailed treatment of all of the rejections please consult the Final rejection dated 8/3/2005 herein enclosed.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Venkat Perungavoor

Art Unit 2132

Conferees:

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Gilberto Barro´n Jr

JUSTIN T. DARROW
PRIMARY EXAMINER

Justin Darrow

DETAILED ACTION

Response to Arguments

1. The Examiner mentions that Claim 8 and 15 are rejected under 35 USC § 102(e) to U.S. Patent 6,279,113 to Vaidya.

2. The objection to the specifications is withdrawn as the application contained blanks with reference to related applications, but are remedied by filling them in.

3. The Applicant's arguments regarding Claim 1 are not persuasive. As Vaidya discloses monitoring all seven layers of the OSI model see Col 4 Ln 28-33. And further it is commonly known in the art that the OSI model includes sever layers(Physical, Data Link, Network, Transport, Session, Presentation, Application[1]) which includes the present invention's monitoring of application, transport and network.

4. The Applicant's arguments regarding Claim 17 are not persuasive. As Holland does disclose a network stack containing a protocol driver, a media access control driver and a intrusion prevention system transport service provider layer see Col 5 Ln 9-21 & Col 6 Ln 62-65 & Col 4 Ln 52-58 & Fig. 5 item 121. Holland discloses the drivers(media access and protocol drivers) being stored in a memory space and further discloses an IP stack where information regarding

[1] See http://webopedia.internet.com/quick_ref/OSI_Layers.asp for more details.

layers are stored; as stated earlier transport layer of the intrusion detection system(TCP/UDP) see Col 6 Ln 47-61.

5. And further the Examiner reminds the Applicants, *In Syntex (U.S.A.) LLC V. Apotex Inc.,* 74 USPQ2d 1823 (CA FC 2005), "Prior art reference teaches away from claimed invention if it suggests that developments flowing from its disclosures are unlikely to produce objective of invention, and what reference teaches person of ordinary skill in art is not limited to what reference specifically 'talks about' or what is specifically 'mentioned' or 'written' in reference;..."

6. For citations of 35 USC § 102(e) and 35 USC § 103(a) please consult please office action.

Response to Amendment

Claim Rejections - 35 USC § 102

7. Claim 1, 5-9, 15-16 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 62791 13 to Vaidya.

8. Regarding Claim 1 , Vaidya discloses the an intrusion detection system whereby the all the seven OSI layers are monitored; which includes the application, transport and network layer see Col 4 Line 29-31 .(see discussion above relating to arguments)

9. Regarding Claim 5, Vaidya discloses the first layer(application layer) interfacing with the file system. Vaidya discloses having an memory of profiles and this profile interfacing with application session see Col 4 Line 8-10 & Line 19-22.

10. Regarding Claim 6, Vaidya discloses the file system interfacing with the first layer which includes an database for storing repods and signature file see Col 3 Line 66- Col 4 Line 39.

11. Regarding Claim 7, Vaidya discloses the first layer(application layer) providing the third layer(network layer) the signature files see Col 3 Line 40-48.

12. Regarding Claim 8, Vaidya discloses the communication session between intrusion prevention system and database system see Col 2 Line 30-53.

13. Regarding Claim 9, Vaidya discloses the an intrusion detection system whereby the all the seven OSI layers are monitored, which includes the application, transport and network layer see Col 4 Line 29-31 . Vaidya also discloses the instructions and processor see Col 6 Line 1 1-25.

14. Claim 15 is rejected under the same rationale as Claim 8 above.

15. Regarding Claim 16, Vaidya discloses the archiving of intrusion related events in a database file system see Col 4 Line 8-18 & Col 5 Line 47-51.

Claim Rejections - 35 USC § 103

16. Claim 2, 3, 4,10-13, 17-19 rejected under 35 U.S.C. 1O3(a) as being unpatentable over U.S. Patent 6279113 to Vaidya in view of U.S. 6851061 B1 to Holland 111 et al .

17. Regarding 2, 3 and 4, Vaidya does not disclose the use of drivers to monitor network layer, transport layer interface and first layer interfacing with the second layer by a dynamically linked library. However, Holland et al. discloses the use of filter to monitor the network layer see Column 4 Line 52-67., further discloses the use of an audit system to monitor transport layer see Column 4 Line 31-52., and also discloses the use of dynamically linked library for interfacing with the first and second layer see Col 5 Line 61-Col 6 Line 15.It would be obvious to one having ordinary skill in the ad at the time of the invention to include use of drivers to monitor network layer, transport layer interface and first layer interfacing with the second layer by a dynamically linked library in the invention of Vaidya in order to increase internal security and latency as taught in Holland see Col 4 Line 2-19.

18. Regarding Claim 10,12, and 13, are rejected under the same rationale as Claim 2, 3 and 4 above.

19. Regarding Claim 11, Vaidya does not disclose the initialization of stack. However, Holland et al. discloses the initialization see Col 4 Line 43-67. It would be obvious to one having ordinary skill in the art at the time of the invention to include initialization of stack in the invention of Vaidya in order to have an clean stack for data to be put upon.

20. Regarding Claim 17, Vaidya discloses an processor, memory module see Column 6 Line 1-26 & Col 5 Line 47-67, but does not disclose the use of drivers to monitor network layer, transport layer interface and first layer interfacing with the second layer by a dynamically linked library. However, Holland et al. discloses the use of filter to monitor the network layer see Column 4 Line 52-67, further discloses the use of an audit system to monitor transport layer see Column 4 Line 31-52, and also discloses the use of dynamically linked library for interfacing with the first and second layer see Col 5 Line 61-Col 6 Line 15.It would be obvious to one having ordinary skill in the ad at the time of the invention to include use of drivers to monitor network layer, transport layer interface and first layer interfacing with the second layer by a dynamically linked library in the invention of Vaidya in order to increase internal security and latency as taught in Holland see Col 4 Line 2-19.(see discussion above relating to arguments)

21. .Regarding Claim 18, Vaidya discloses the intrusion protection system communicating with the file system see Col 5 Line 27-33.

22. Regarding Claim 19, Vaidya discloses the logging of intrusion-related data in database for future reference see Col 5 Line 47-50.

Conclusion

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkatanarayanan Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on

8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Venkatanarayanan Perungavoor
Examiner
Art Unit 2132

7/28/2005